(12) UK Patent Application (19) GB (11) 2 324 682 (13) A

(43) Date of A Publication 28.10.1998

(21) Application No 9802113.2

(22) Date of Filing 30.01.1998

(30) Priority Data
(31) 09071989 (32) 31.01.1997 (33) JP

(71) Applicant(s)
NEC Corporation
(Incorporated in Japan)
7-1,Shiba 5-Chome, Minato-Ku, Tokyo, Japan

(72) Inventor(s)
Keiichi Hayashi
Hiroto Nagai

(74) Agent and/or Address for Service
Mathys & Squire
100 Grays Inn Road, LONDON, WC1X 8AL,
United Kingdom

(51) INT CL^6
G06F 1/00 , H04L 9/22 9/32 // H04Q 7/22

(52) UK CL (Edition P)
H4L LDGX L1H10
H4P PDCSA PDCSP

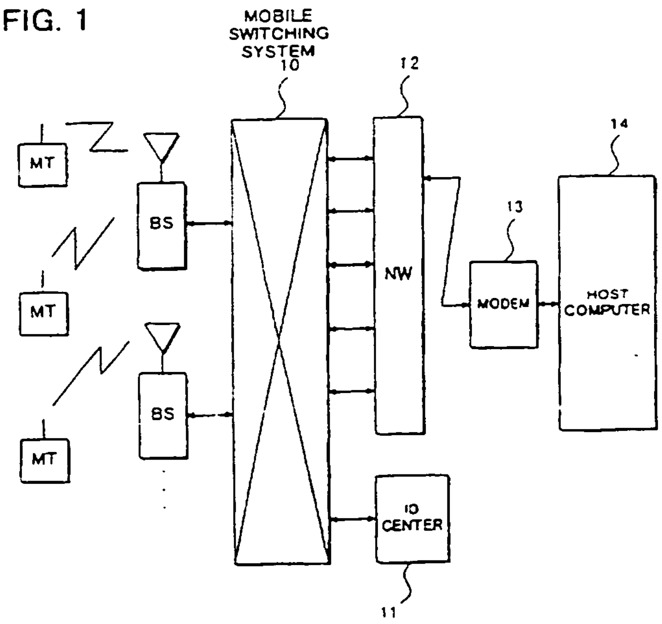
(56) Documents Cited
WO 98/11487 A1 JP 040023527 A SE 000503752 A

(58) Field of Search
UK CL (Edition P) **H4L LDGX LDSK , H4P PDCSA**
INT CL^6 **G06F 1/00 , H04Q 7/22 7/24 7/38**
Online: WPI

(54) Abstract Title
Connection of a mobile wireless terminal to a host computer

(57) A connection is established between a wireless mobile terminal and a host computer via a radio mobile communication network. A connection establishment request, which may be encrypted, is sent from the mobile to the host computer. If the information sent in the request is verified, a response is sent back to the mobile to establish the connection. The encrypted data may be different each time a connection request is made and may include the time the call is made. A hash value may be generated using the encryption data, a random number generator initialised depending on the hash value, and a random number generated from the time information.

FIG. 1



GB 2 324 682 A

FIG. 1

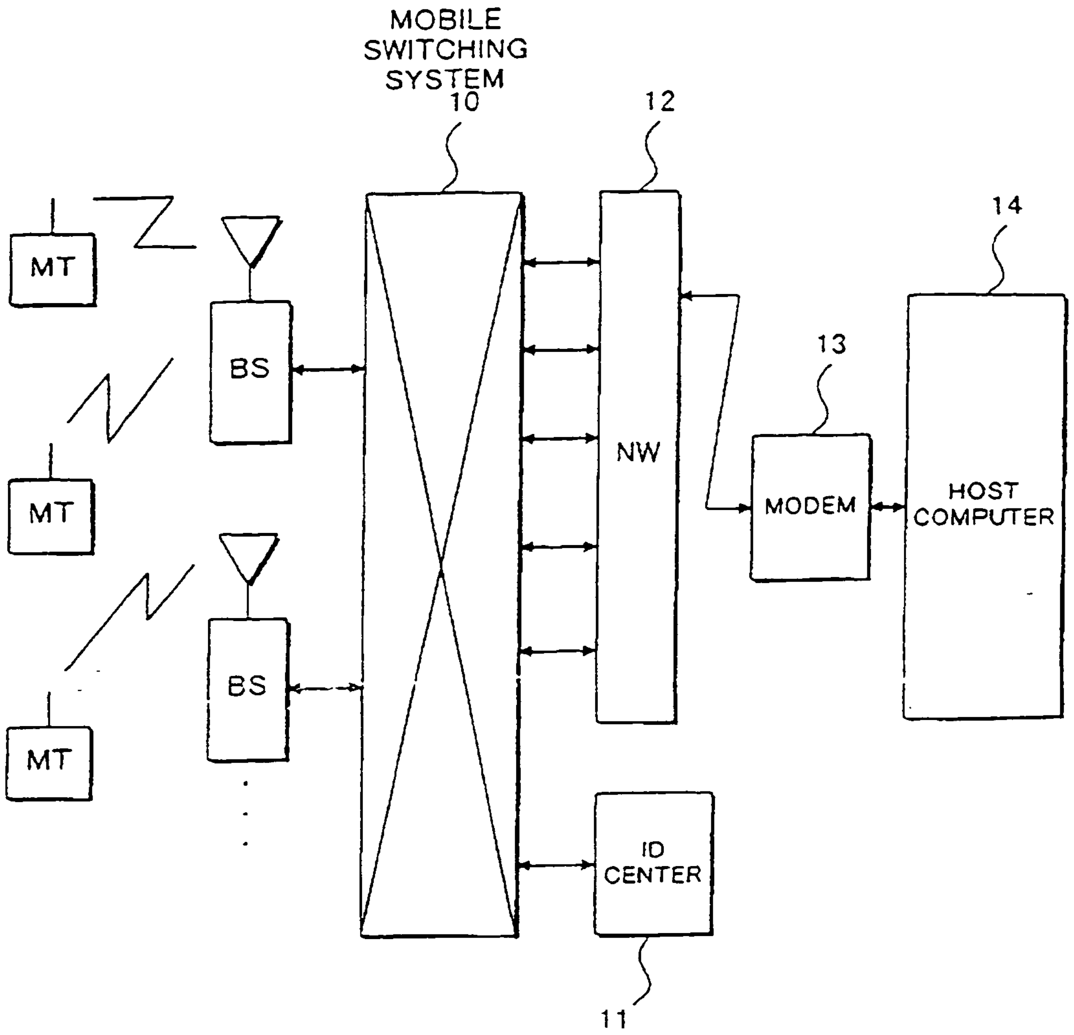

MOBILE
SWITCHING
SYSTEM
10
12
14
MT
BS
MT
BS
MT
NW
13
MODEM
HOST
COMPUTER
ID
CENTER
11

FIG. 2

MOBILE TERMINAL

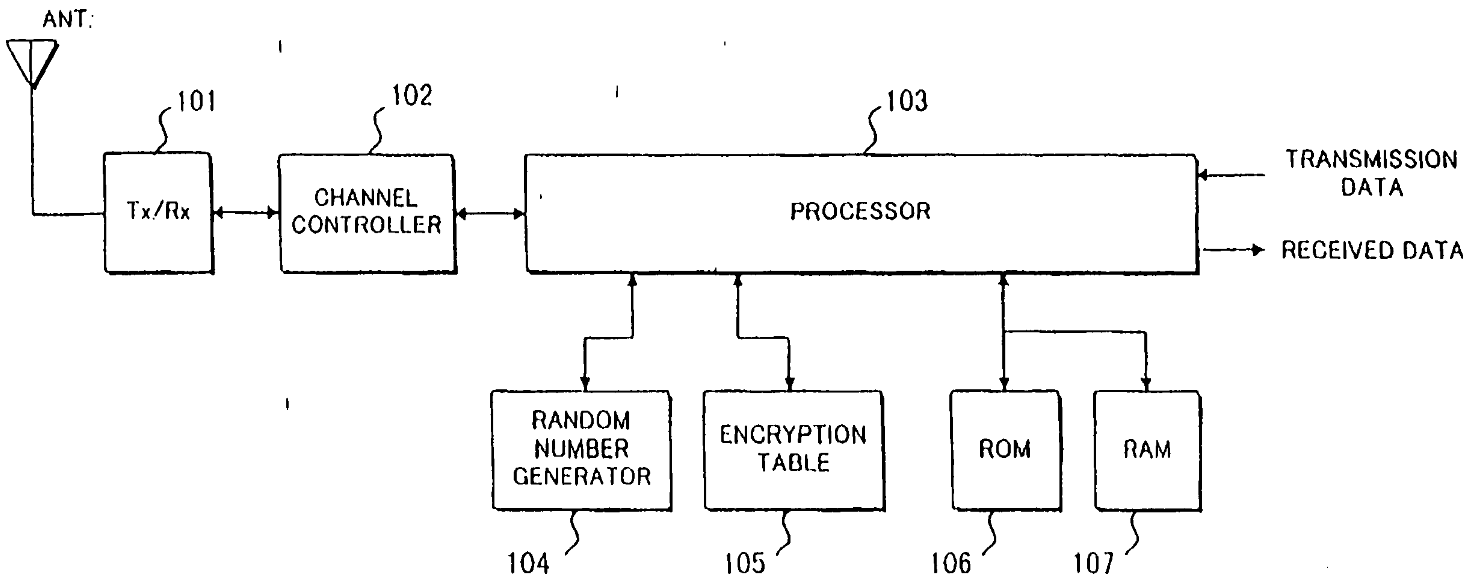


FIG. 3

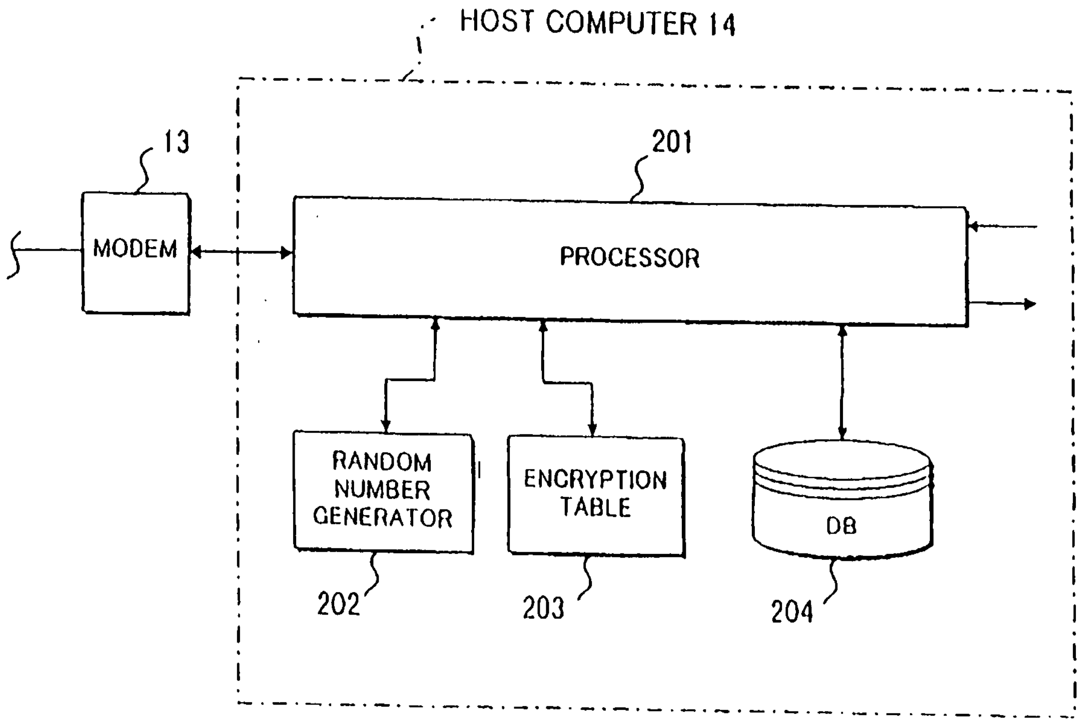

HOST COMPUTER 14
13
MODEM
201
PROCESSOR
RANDOM NUMBER GENERATOR
202
ENCRYPTION TABLE
203
DB
204

FIG. 4

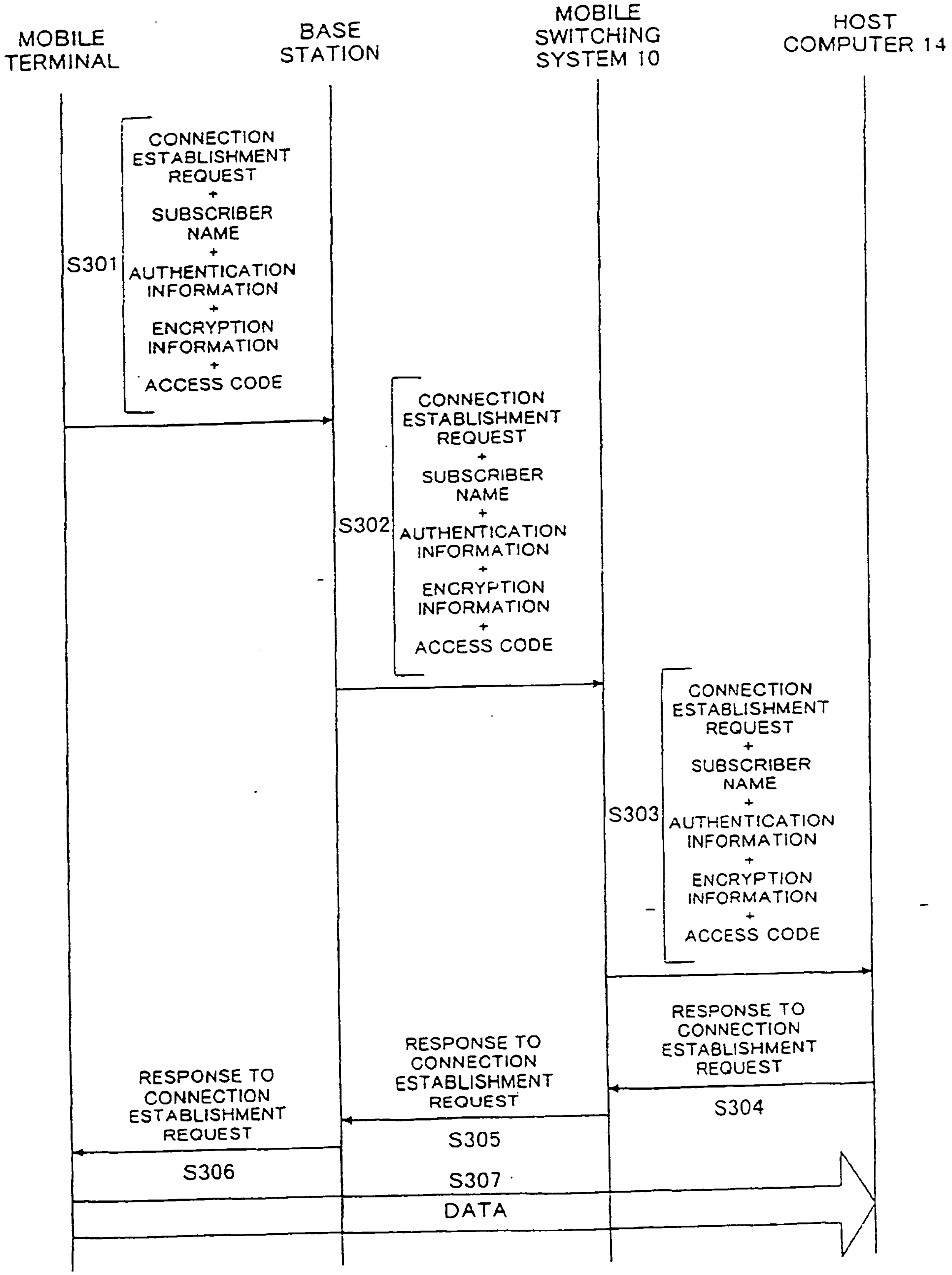

MOBILE TERMINAL
BASE STATION
MOBILE SWITCHING SYSTEM 10
HOST COMPUTER 14
S301
CONNECTION ESTABLISHMENT REQUEST + SUBSCRIBER NAME + AUTHENTICATION INFORMATION + ENCRYPTION INFORMATION + ACCESS CODE
S302
CONNECTION ESTABLISHMENT REQUEST + SUBSCRIBER NAME + AUTHENTICATION INFORMATION + ENCRYPTION INFORMATION + ACCESS CODE
S303
CONNECTION ESTABLISHMENT REQUEST + SUBSCRIBER NAME + AUTHENTICATION INFORMATION + ENCRYPTION INFORMATION + ACCESS CODE
RESPONSE TO CONNECTION ESTABLISHMENT REQUEST
S304
RESPONSE TO CONNECTION ESTABLISHMENT REQUEST
S305
RESPONSE TO CONNECTION ESTABLISHMENT REQUEST
S306
S307
DATA

FIG. 5

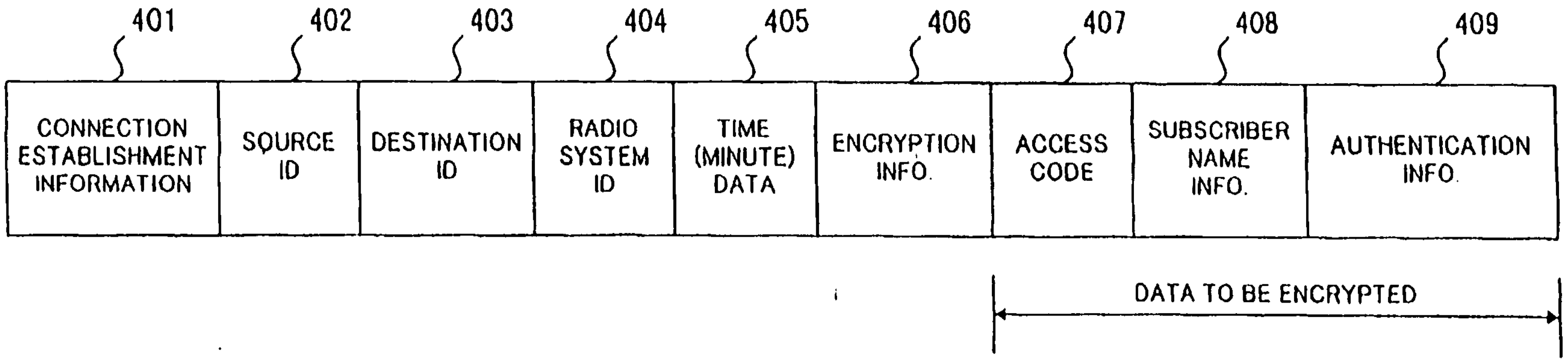

401
CONNECTION ESTABLISHMENT INFORMATION
402
SOURCE ID
403
DESTINATION ID
404
RADIO SYSTEM ID
405
TIME (MINUTE) DATA
406
ENCRYPTION INFO.
407
ACCESS CODE
408
SUBSCRIBER NAME INFO.
409
AUTHENTICATION INFO.
DATA TO BE ENCRYPTED

FIG. 6

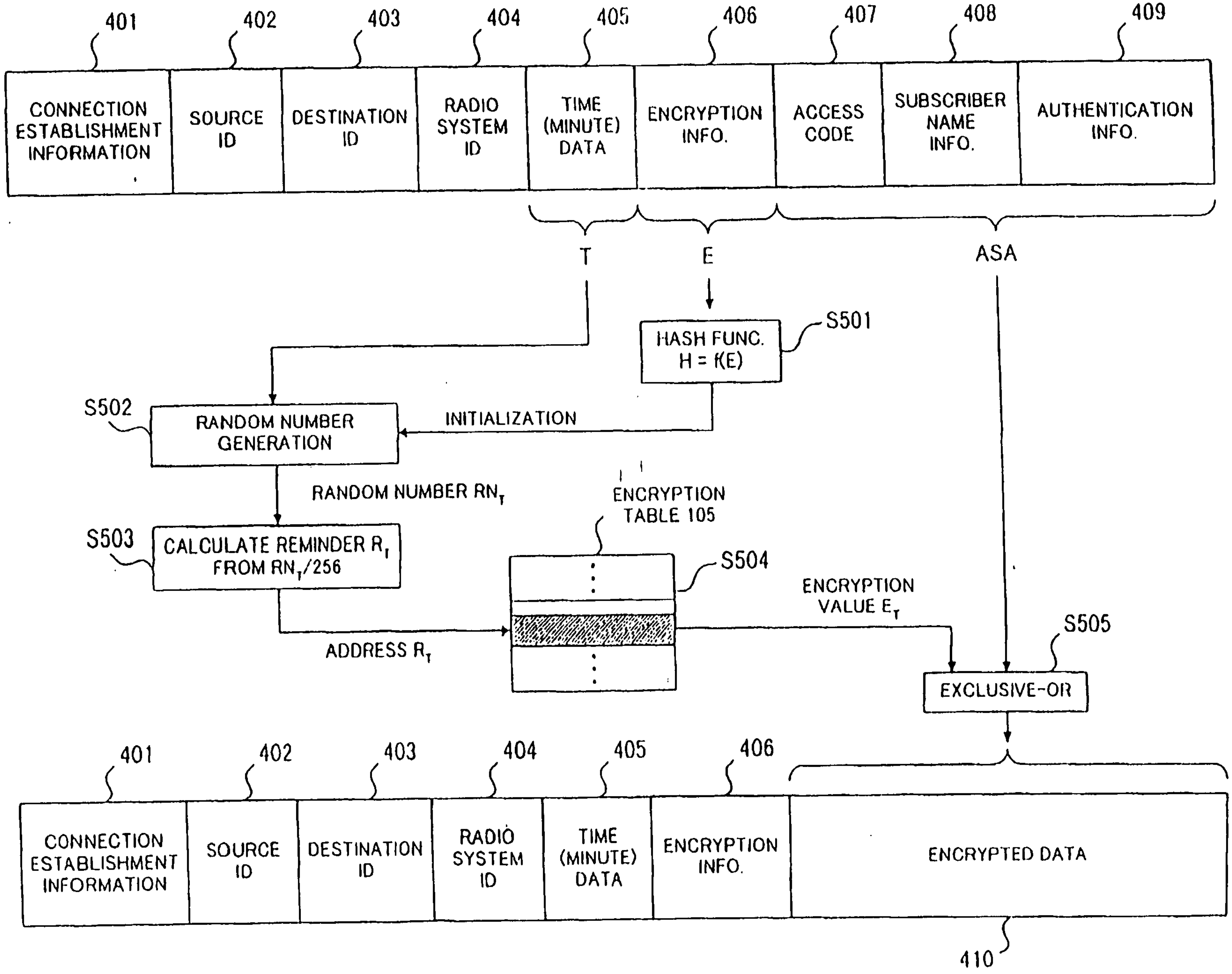
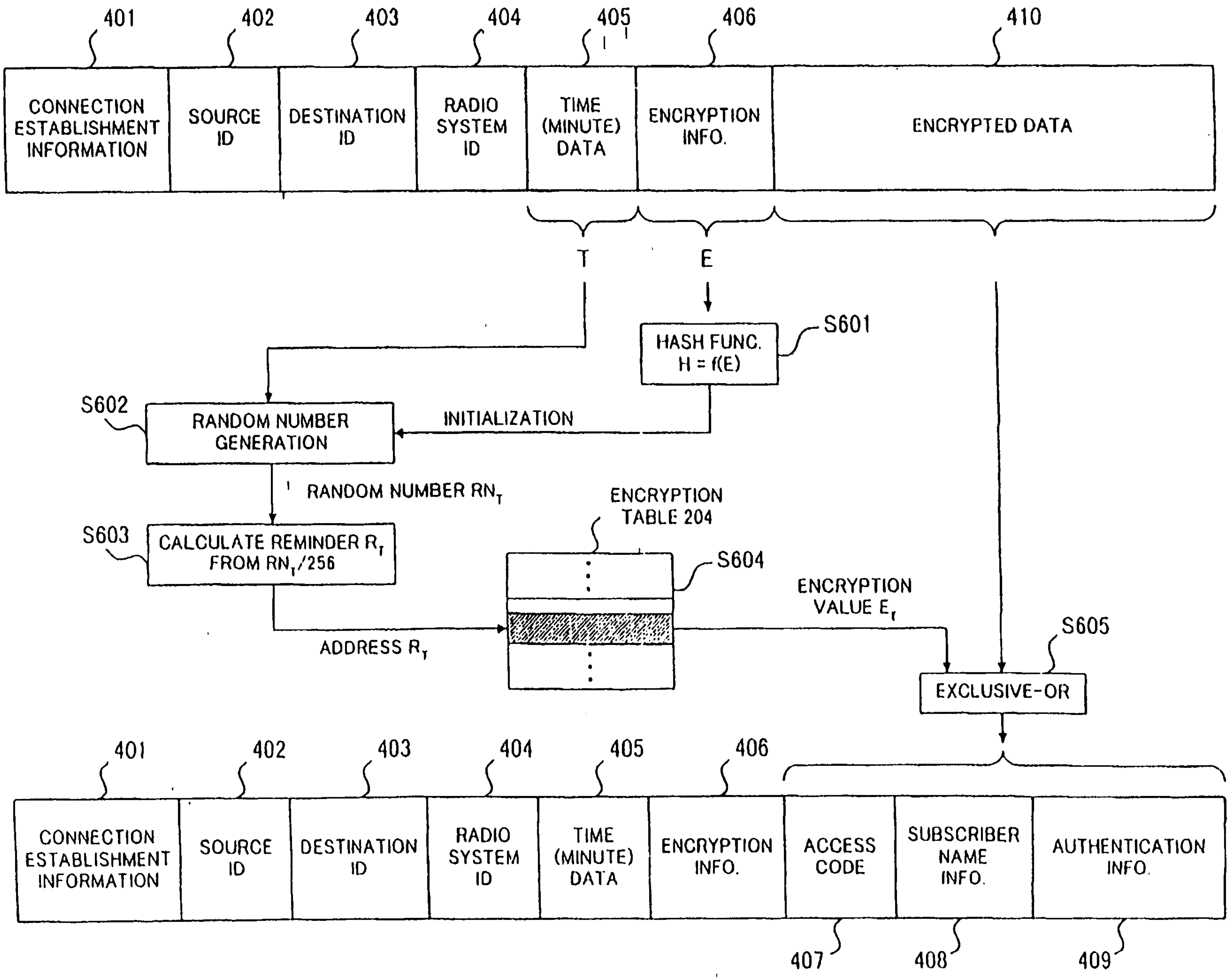

401
402
403
404
405
406
407
408
409
CONNECTION ESTABLISHMENT INFORMATION
SOURCE ID
DESTINATION ID
RADIO SYSTEM ID
TIME (MINUTE) DATA
ENCRYPTION INFO.
ACCESS CODE
SUBSCRIBER NAME INFO.
AUTHENTICATION INFO.
T
E
ASA
HASH FUNC. H = f(E)
S501
S502
RANDOM NUMBER GENERATION
INITIALIZATION
RANDOM NUMBER RN_T
S503
CALCULATE REMINDER R_T FROM $RN_T/256$
ENCRYPTION TABLE 105
S504
ADDRESS R_T
ENCRYPTION VALUE E_T
S505
EXCLUSIVE-OR
401
402
403
404
405
406
CONNECTION ESTABLISHMENT INFORMATION
SOURCE ID
DESTINATION ID
RADIO SYSTEM ID
TIME (MINUTE) DATA
ENCRYPTION INFO.
ENCRYPTED DATA
410

FIG. 7


401
402
403
404
405
406
410
CONNECTION ESTABLISHMENT INFORMATION
SOURCE ID
DESTINATION ID
RADIO SYSTEM ID
TIME (MINUTE) DATA
ENCRYPTION INFO.
ENCRYPTED DATA
T
E
HASH FUNC. H = f(E)
S601
S602
RANDOM NUMBER GENERATION
INITIALIZATION
RANDOM NUMBER RN_T
S603
CALCULATE REMINDER R_T FROM $RN_T/256$
ENCRYPTION TABLE 204
S604
ENCRYPTION VALUE E_T
ADDRESS R_T
S605
EXCLUSIVE-OR
401
402
403
404
405
406
CONNECTION ESTABLISHMENT INFORMATION
SOURCE ID
DESTINATION ID
RADIO SYSTEM ID
TIME (MINUTE) DATA
ENCRYPTION INFO.
ACCESS CODE
SUBSCRIBER NAME INFO.
AUTHENTICATION INFO.
407
408
409

WIRELESS MOBILE COMMUNICATIONS SYSTEM

The present invention generally relates to a method of establishing a connection between a wireless mobile terminal and a host computer in a wireless mobile communications system, and to such a wireless mobile communication system, a wireless mobile terminal, a host computer and also encryption and decryption methods in such a wireless mobile communication system, and in particular to an access method which provides a mobile terminal with access to a host computer of the mobile terminal through the mobile communications.

In radio mobile communications, a plurality of data exchanges are needed for establishing connection between a mobile terminal and a connection control station. To achieve rapid connection establishment, there has been proposed a call connection procedure in Japanese Patent Unexamined Publication No 4-23527. More specifically, when calling, the mobile terminal transmits a calling signal conveying a source ID (identification) number, a destination ID number, and additional information to the connection control, the following processes are performed concurrently: a subscriber information check using the source ID number, an additional information check, and a connection process of a switching system. Only when all responses to the checks and the connection process are affirmative, the connection between the mobile terminal and the connection control station is established.

An authentication method using secret-key encryption has been proposed in Japanese Patent Unexamined Publication No. 5-183507. An ID center transmits random data as an authentication request signal to a mobile terminal. At the mobile terminal, the received random data and a secret key input by the subscriber are used to produce encrypted data. The encrypted data is transmitted as an authentication response signal to the ID center. At the ID center, the random data and a registered secret key are used to produce encrypted data which is compared with the received encrypted data from the mobile terminal. If the produced encrypted data is coincident with the received one, the authentication check is affirmative.

Similarly, a radio telephone service access method using secret-key encryption has been proposed in Japanese Patent Unexamined Publication No. 4-2333341.

In the case of a host access system in which a mobile terminal obtains access to a host computer through the mobile communication system, however, the conventional technique described above fails to provide both sufficiently rapid connection establishment and sufficient security of private information. In the connection control procedure where a calling signal conveying a source ID number, a destination ID number and additional information is transmitted to the connection control station, after all the necessary check processes have been completed in the mobile communication system, the connection between the mobile terminal and the host computer is established. In other words, the connection cannot be established without completing all the necessary check processes in the mobile communication system.

In the conventional authentication methods using secret-key encryption, a plurality of data exchanges are needed for connection establishment between a mobile terminal and a connection control station. Therefore, it is very difficult to shorten the time required for connection establishment.

An object of at least the preferred embodiment of the present invention is to provide a method and system which can effectively perform connection establishment at a short time.

Another such object is to provide a method which can achieve rapid connection establishment with data security.

In a first aspect, the present invention provides a method of establishing a connection between a wireless mobile terminal and a host computer in a wireless mobile communications system, comprising the steps of at the wireless mobile terminal, producing a connection establishment request signal including first information which is required to obtain services from the host computer, and transmitting the connection establishment request signal to the host computer, at the host computer receiving the connection establishment request signal from the wireless mobile terminal, verifying the first information included in the connection establishment request signal received, and transmitting a response signal back to the wireless mobile terminal to establish the connection between the wireless mobile terminal and the host computer only when the first information has been verified.

According to the above, when establishing a connection between a wireless mobile terminal and a host computer in a wireless mobile communications system, the wireless mobile terminal produces a connection establishment request signal including first information which is required to obtain services from the host computer and then transmits the connection establishment request signal to the host computer. When receiving the connection establishment request signal from the wireless mobile terminal, the host computer verifies the first information included in the connection establishment request signal received, and transmits a response signal back to the wireless mobile terminal only when the first information has been verified. This causes the connection to be established between the wireless mobile terminal and the host computer.

The wireless mobile terminal may encrypt the first information into encrypted data according to a predetermined encryption scheme and produce the connection establishment request signal which includes the encrypted data in place of the first information. Similarly, the host computer may decrypt the encrypted data included in the connection establishment request signal received into the first information according to the predetermined encryption scheme and verify the first information.

The first information may be encrypted into different encrypted data each time the connection establishment request signal is transmitted.

The present invention also provides a wireless mobile communications system comprising a plurality of wireless mobile terminals, a plurality of wireless base stations and a host computer, wherein a connection is established between a wireless mobile terminal and a host computer through a wireless base station, the wireless mobile terminal comprising a wireless transceiver for communicating with the wireless base station, and a terminal processor for producing a connection establishment request signal including first information which is required to obtain services from the host computer and controlling the wireless transceiver such that the connection establishment request signal is transmitted to the host computer, and the host computer comprising a transceiver connected to a switched network and a host processor for verifying the first information included in the connection establishment request signal received from the wireless mobile terminal and controlling the transceiver such that a response signal is transmitted back to the wireless mobile terminal to establish the connection between the wireless mobile terminal and the host computer only when the first information has been verified.

The present invention extends to a wireless mobile terminal for establishing a connection with a host computer connected to a stationary network system through a wireless mobile communications system, comprising a wireless transceiver for communicating with a nearby wireless base station of the wireless mobile communications system, and a processor for producing a connection establishment request signal including first information which is required to obtain services from the host computer, encrypting the first information into encrypted data according to a predetermined encryption scheme, and controlling the wireless transceiver such that the connection establishment request signal including the encrypted data in place of the first information is transmitted to the host computer, wherein the connection is established between the wireless mobile terminal and the host computer when a response signal to the connection establishment request signal is received from the host computer.

The present invention also extends to a host computer connected to a stationary switched network which is in turn connected to a wireless mobile communications system, comprising a transceiver connected to the stationary switched network, the transceiver receiving a connection establishment request signal from a wireless mobile terminal, the connection establishment request signal including encrypted data which is obtained by encrypting first information according to a predetermined encryption scheme, the first information being required to obtain services from the host computer, and a processor for decrypting the encrypted data included in the connection establishment request signal received into the first information according to the predetermined encryption scheme, verifying the first information included in the connection establishment request signal, and controlling the transceiver such that a response signal is transmitted back to the wireless mobile terminal to establish the connection between the wireless mobile terminal and the host computer only when the first information has been verified.

In another aspect, the present invention provides a method of encrypting a part of a transmission signal in a wireless mobile communications system, comprising the steps of producing a transmission signal including first information to be encrypted, encryption information, and time information which indicates when the transmission signal is transmitted, generating a random number based on the encryption information and the time information, converting the random number to an encryption address value having a predetermined number of digits, reading an encryption value from an encryption table depending on the encryption address value, and encrypting the first information by combining the encryption value and the first information.

In yet another aspect, the present invention provides a method of decrypting a part of a reception signal in a wireless mobile communications system comprising the steps of receiving a reception signal including encrypted data to be decrypted, encryption information, and time information which indicates when the reception signal is transmitted at a transmitting side, generating a random number based on the encryption information and the time information, converting the random number to an encryption address value having a predetermined number of digits, reading an encryption value from an encryption table depending on the encryption address value, and decrypting the encrypted data by combining the encryption value and the encrypted data.

Preferred features of the present invention will now be described, purely by way of example only, with reference to the accompanying drawings, in which:-

Fig. 1 is a schematic block diagram showing the configuration of a network system implementing an access method;

Fig. 2 is a block diagram showing the schematic internal circuit of a mobile terminal in the network system of Fig. 1;

Fig. 3 is a block diagram showing the schematic internal circuit of a host computer in the network system of Fig. 1;

Fig. 4 is a diagram showing a sequence for connection establishment ;

Fig. 5 is a diagram showing the signal format of a calling signal from a mobile terminal;

Fig. 6 is a diagram showing an operation of an encryption process ; and

Fig. 7 is a diagram showing an operation of a decryption process..

Referring to Fig. 1, a plurality of mobile terminals each labeled MT are possessed by registered subscribers, respectively. A plurality of base stations each labeled BS form radio zones, respectively. Each base station can communicate with each mobile terminal located therein through a radio channel. The base stations are connected to a mobile switching system 10 which is further connected to an ID center 11 and a stationary switched network 12 such as public switched telephone network.

A host computer 14 is connected to the stationary switched network 12 through a modem 13 or a set of digital service unit (DSU) and a terminal adapter (TA). Assuming that a mobile terminal MT is registered as a subscriber to the host computer 14, the mobile terminal MT can access to the host computer 14 through the mobile switching system 10 and the stationary switched network 12 according to an access procedure as will be described later.

Referring to Fig. 2, each mobile terminal MT is provided with a radio system 101 which receives and transmits a radio signal from and to a nearby base station through an antenna. The mobile terminal MT is further provided with a processor 103 performs the operation control of the mobile terminal. The processor 103 performs encryption/decryption processing using a random number generator 104 and an encryption table 105 to encrypt a predetermined part of transmission data and to decrypt received data. The operation control of the mobile terminal is performed using a ROM 106 and a RAM 107. The ROM 106 stores necessary programs and the subscriber ID number which was uniquely assigned to the mobile terminal MT. In the case of a mobile telephone, a speaker, a microphone, a display, and a keypad are further provided as a user interface.

Referring to Fig. 3, the host computer 14 is provided with a processor 201 which performs encryption/decryption processing using a random number generator 202 and an encryption table 203 to decrypt a predetermined part of received data from the mobile terminal MT and to encrypt transmission data. The random number generator 202 and the encryption table 203 are the same as those of the mobile terminal MT. The processor 201 performs the operation control of the authentication procedure using a database 204 which stores terminal data, subscriber data and other necessary data for authentication and connection establishment.

ACCESS SEQUENCE

Referring to Fig. 4, in the case where the mobile terminal MT is located in the radio zone of the nearby base station BS and requests connection establishment to the host computer 14, the processor 103 of the mobile terminal MT produces a connection establishment request signal conveying necessary information for communication with the host computer 14 as shown in Fig. 5. The necessary information includes subscriber name information, authentication information, encryption information and an access code as will be described in detail. A predetermined part of the connection establishment request signal is encrypted by the processor 103 using the random number generator 104 and the encryption table 105 and then the connection establishment request signal conveying encrypted data is transmitted to the nearby base station BS through a predetermined radio channel (step S301).

When receiving the connection establishment request signal from the mobile terminal MT, the base station BS transfers it to the mobile switching system 10 (step S302). If it is determined that the mobile terminal MT is a subscriber of the mobile communications system by the ID center 11 checking the ID number conveyed by the connection establishment request signal, the connection establishment request signal is transmitted to the stationary switched network 12. According to the destination ID number included in the connection establishment request signal, the stationary switched network 12 transfers it to the host computer 14 (step S303).

When receiving the connection establishment request signal including the encrypted data from the mobile terminal MT through the stationary switched network 12, the processor 201 of the host computer 14 decrypts the encrypted data and transfers the decrypted data to the processor 201. The processor 201 verifies the subscriber name information and the authentication information by referring to the database 204.

Only when the subscriber name information and the authentication information have been verified, the processor 201 produces a response to the connection establishment request and transmits it to the mobile switching system 10 through the stationary switched network 12 (step S304). The response is transferred from the mobile switching system 10 to the base station BS (step S305) and is further transferred from the base station BS to the mobile terminal MT through a radio channel (step S306).

In this manner, the connection between the mobile terminal MT and the host computer 14 is established and the mobile terminal

MT can transmit data to the host computer 14 through the established connection (step S307). Since the necessary information is transmitted to the host computer 14 and the response to the connection establishment request is transmitted back to the mobile terminal MT when the necessary information has been verified, the connection can be established by only one data transmission-reception between the mobile terminal MT and the host computer 14. Therefore, the connection establishment is effectively performed at a short time. Further, only one data transmission-reception causes the reduced possibility that the connection fails to be established due to radio channel impairment conditions.

CONNECTION ESTABLISHMENT REQUEST SIGNAL

Referring to Fig. 5, the connection establishment request signal conveys the following information: connection establishment information 401, source ID number 402, destination ID number 403, radio system ID number 404, time data 405, encryption information 406, access code 407, subscriber name information 408 and authentication information 409. The source ID number 402 is the identification number of the mobile terminal MT and the destination ID number is the subscriber number of the host computer 14.

The time data 405 indicates the time of day when the mobile terminal MT makes a call. In this embodiment, the time data 405 indicates the minute of the time of day. The access code 407 is used to identify the access means and the type of the mobile terminal MT. More specifically, according to the access code 407 conveyed by the connection establishment request signal, the host computer 14 changes the connection establishment process to the procedure corresponding to the mobile terminal MT. The subscriber name information 408 is the ID number of the subscriber which possesses the mobile terminal MT.

To protect against tapping, a set of the access code 407, the subscriber name information 408 and the authentication information 409 (called ASA data, hereinafter) is encrypted and transmitted as will be described hereinafter.

ENCRYPTION

As shown in Fig. 6, the processor 103 of the mobile terminal MT reads the encryption information 406 (here, value E) and the time (minute) data 405 (here, value T) from the connection establishment request signal. The processor 103 calculates a Hash value H from the value E using the Hash function: H = f(E) (step S501).

The processor 103 initializes the random number generator 104 according to the Hash value H and then obtains a random number RN_T from the random number generator 104 according to the value T of the time (minute) data 405 (step S502). Further, the processor 103 converts the random number RN_T to a number R_T ranging from 0 to 255 by dividing the random number RN_T by 256 to obtain the reminder R_T thereof (step S503).

Subsequently, the processor 103 reads encryption value E_T from the location of the encryption table 105 which is addressed with the reminder R_T. Finally, the processor 103 exclusive-ORs the encryption value E_T and the ASA data of the access code 407, the subscriber name information 408 and the authentication information 409 to produce encrypted data 410 (S505). In this manner, the processor 103 produces the connection establishment request signal including the encrypted data 410 which is to be transmitted to the host computer 14.

DECRYPTION

As shown in Fig. 7, when receiving the connection establishment request signal including the encrypted data 410 from the mobile terminal MT, the processor 201 of the host computer 14 reads the encryption information 406 (here, value E) and the time (minute) data 405 (here, value T) from the received connection establishment request signal. The processor 201 calculates a Hash value H from the value E using the Hash function: $H = f(E)$ (step S601).

The processor 201 initializes the random number generator 202 according to the Hash value H and then obtains a random number RN_T from the random number generator 202 according to the value T of the time (minute) data 405 (step S602). Further, the processor 201 converts the random number RN_T to a number R_T ranging from 0 to 255 by dividing the random number RN_T by 256 to obtain the reminder R_T thereof (step S603).

Subsequently, the processor 201 reads encryption value E_T from the location of the encryption table 203 which is addressed with the reminder R_T. Finally, the processor 201 exclusive-ORs the encryption value E and the encrypted data to reproduce the original set of the access code 407, the subscriber name information 408 and the authentication information 409. In this manner, the processor 201 produces the original connection establishment request signal.

Since the data to be secret is encrypted and then transmitted from the mobile terminal MT to the host computer 14, the data security is maintained.

Each feature disclosed in this specification (which term includes the claims) and/or shown in the drawings may be incorporated in the invention independently of other disclosed and/or illustrated features.

The text of the abstract filed herewith is repeated below as part of the specification.

In a network system including a wireless mobile communications system, when establishing a connection between a wireless mobile terminal and a host computer connected to a stationary network system, the wireless mobile terminal produces a connection establishment request signal including first information which is required to obtain services from the host computer and then transmits the connection establishment request signal to the host computer. The host computer verifies the first information included in the connection establishment request signal received from the wireless mobile terminal and transmits a response signal back to the wireless mobile terminal only when the first information has been verified. This causes the connection to be established between the wireless mobile terminal and the host computer.

CLAIMS

1. A method of establishing a connection between a wireless mobile terminal and a host computer in a wireless mobile communications system, comprising the steps of:

at the wireless mobile terminal,

a) producing a connection establishment request signal including first information which is required to obtain services from the host computer; and

b) transmitting the connection establishment request signal to the host computer;

at the host computer,

c) receiving the connection establishment request signal from the wireless mobile terminal;

d) verifying the first information included in the connection establishment request signal received; and

e) transmitting a response signal back to the wireless mobile terminal to establish the connection between the wireless mobile terminal and the host computer only when the first information has been verified.

2. A method according to claim 1, wherein the step a) comprises the steps of:

encrypting the first information into encrypted data according to a predetermined encryption scheme; and producing the connection establishment request signal which includes the encrypted data in place of the first information, and

the step d) comprises the steps of:

decrypting the encrypted data included in the connection establishment request signal received into the first information according to the predetermined encryption scheme: and

verifying the first information.

3. A method according to claim 2, wherein the first information is encrypted into different encrypted data each time the connection establishment request signal is transmitted.

4. A method according to claim 1, wherein

the connection establishment request signal further includes calling time data and encryption information, and

the first information includes subscriber identification information and authentication information.

5. A method according to claim 4, wherein

the step a) comprises the steps of:

encrypting the first information into encrypted data based on the calling time data and the encryption information according to a predetermined encryption scheme; and

producing the connection establishment request signal which includes the encrypted data in place of the first the host computer comprising:

a transceiver connected to a switched network; and

a host processor for verifying the first information included in the connection establishment request signal received from the wireless mobile terminal and controlling the transceiver such that a response signal is transmitted back to the wireless mobile terminal to establish the connection between the wireless mobile terminal and the host computer only when the first information has been verified.

7. A wireless mobile communications system according to claim 6, wherein

the wireless mobile terminal further comprises:

a terminal processor for encrypting the first information into encrypted data according to a predetermined encryption scheme and producing the connection establishment request signal which includes the encrypted data in place of the first information, and

the host computer further comprising:

a host processor for decrypting the encrypted data included in the connection establishment request signal received into the first information according to the predetermined encryption scheme.

8. A wireless mobile communications system according to claim 7, wherein

the terminal processor comprises a random number generator and an encryption table for the predetermined encryption scheme, and

the host processor comprises the same random number generator and the same encryption table as those of the terminal processor.

9. A wireless mobile communications system according to claim 7, wherein the first information is encrypted into different encrypted data each time the connection establishment request signal is transmitted.

10. A wireless mobile terminal for establishing a connection with a host computer connected to a stationary network system through a wireless mobile communications system, comprising:

a wireless transceiver for communicating with a nearby wireless base station of the wireless mobile communications system; and

a processor for producing a connection establishment request signal including first information which is required to obtain services from the host computer, encrypting the first information into encrypted data according to a predetermined encryption scheme, and controlling the wireless transceiver such that the connection establishment request signal including the encrypted data in place of the first information is transmitted to the host computer, wherein the connection is established between the wireless mobile terminal and the host computer when a response signal to the connection establishment request signal is received from the host computer.

11. A host computer connected to a stationary switched network which is in turn connected to a wireless mobile communications system, comprising:

a transceiver connected to the stationary switched network, the transceiver receiving a connection establishment request signal from a wireless mobile terminal, the connection establishment request signal including encrypted data which is obtained by encrypting first information according to a predetermined encryption scheme, the first information being required to obtain services from the host computer; and

a processor for decrypting the encrypted data included in the connection establishment request signal received into the first information according to the predetermined encryption scheme, verifying the first information included in the connection establishment request signal, and controlling the transceiver such that a response signal is transmitted back to the wireless mobile terminal to establish the connection between the wireless mobile terminal and the host computer only when the first information has been verified.

12. A wireless mobile terminal according to claim 10, wherein the first information is encrypted into different encrypted data each time the connection establishment request signal is transmitted.

13. A host computer according to claim 11, wherein the first information is encrypted into different encrypted data each time the connection establishment request signal is transmitted.

14. A method of encrypting a part of a transmission signal in a wireless mobile communications system, comprising the steps of:

a) producing a transmission signal including first information to be encrypted, encryption information, and time information which indicates when the transmission signal is transmitted,

b) generating a random number based on the encryption information and the time information;

c) converting the random number to an encryption address value having a predetermined number of digits;

d) reading an encryption value from an encryption table depending on the encryption address value; and

e) encrypting the first information by combining the encryption value and the first information.

15. A method according to claim 14, wherein the step b) comprises the steps of:

generating a Hash value from the encryption information using a Hash function;

initializing a random number generator depending on the Hash value; and

generating the random number from the time information.

16. A decryption method according to claim 14 or 15, wherein in the step e), the first information is encrypted by Exclusive-ORing the encryption value and the first information.

17. A method ~~of~~ decrypting a part of a reception signal in a wireless mobile communications system, comprising the steps of:

a) receiving a reception signal including encrypted data to be decrypted, encryption information, and time information which indicates when the reception signal is transmitted at a transmitting side;

b) generating a random number based on the encryption information and the time information;

c) converting the random number to an encryption address value having a predetermined number of digits;

d) reading an encryption value from an encryption table depending on the encryption address value; and

e) decrypting the encrypted data by combining the encryption value and the encrypted value and the encrypted data.

18. A decryption method according to Claim 17, wherein the step b) comprises the steps of:

generating a Hash value from the encryption information using a Hash function;

initializing a random number generator depending on the Hash value; and

generating the random number from the time information.

19. A decryption method according to Claim 17 or 18, wherein the step e), the encrypted data is decrypted by Excluding-ORing the encryption value and the encrypted data.

20. A method of establishing a connection between a wireless mobile terminal and a host computer in a wireless mobile communications system substantially as herein described with reference to Figure 4 of the accompanying drawings.

21. A wireless mobile communications system substantially as herein described with reference to and as shown in Figures 1 to 3 of the accompanying drawings.

22. A wireless mobile terminal substantially as herein described with reference to and as shown in Figure 2 of the accompanying drawings.

23. A host computer substantially as herein described with reference to and as shown in Figure 3 of the accompanying drawings.

24. A method of encrypting a part of a transmission signal is a wireless mobile communications systems substantially as herein described with reference to Figure 6 of the accompanying drawings.